



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,224	01/16/2002	Mototsugu Nishioka	500.41092X00	4402

24956 7590 02/07/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER

CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 02/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	10/046,224		NISHIOKA ET AL.	
	Examiner		Art Unit	
	David G. Cervetti		2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 November 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 23-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 23-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>11/17/05</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's arguments filed November 17, 2005, have been fully considered but they are not persuasive.
2. Claims 1-22 were cancelled and new claims 23-44 were added, thus claims 23-44 are pending and have been examined.

Response to Amendment

3. The claim objections and rejections of claims 1-22 are withdrawn since the above referenced amendment cancels these claims. Claims 23-44 are examined below.
4. Applicant's arguments fail to comply with 37 CFR 1.111(b) because **they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.** Applicant's argument that "the features of the present invention as recited in the claims are not taught ..." without specifically pointing out the differences between the claimed invention and the prior art of record is not persuasive.
5. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.
6. Cramer et al. (US Patent Number: 6,697,488, hereinafter Cramer) teaches the claimed invention, and suggests the use of a hash function to make the system secure against an adaptive chosen ciphertext after the encryption process and prior to transmission. Thus, at the very least, prior to applying the hash function to the

Art Unit: 2136

ciphertext, Cramer already has the ciphertext ready for transmission as claimed by Applicant. Therefore, the only change needed is to transmit without hashing, which is suggested by Cramer (column 4, lines 19-67, column 5, lines 1-15, column 9, lines 1-67). This change would have been obvious to someone of ordinary skill in the art. Motivations for such change may be found throughout the Art, where a compromise between security and speed or other factors is reached.

7. Furthermore, Abe (Japan Patent 2000-216774) teaches the claimed invention (pages 3-86).

Information Disclosure Statement

8. **The information disclosure statement filed November 17, 2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed.** It has been placed in the application file. Namely, a copy of the document "Non-Malleable Cryptography" was not submitted.

Claim Objections

9. Claims 23-44 are objected to because of the following informalities: there are numerous syntactical errors. Some examples are: "prime number the order of G", open parenthesis without a closing parenthesis, closing parenthesis without an opening parenthesis, "prime number and the order of G", etc.

10. Claim 24 is objected to because of the following informalities: "the number of digits of x)". Appropriate correction is required.

11. Claim 28 is objected to because of the following informalities: "and transmitting (u_1 , u_2 , e , v , C as the ciphertext". Appropriate correction is required.
12. Claim 29 is objected to because of the following informalities: "(new) cryptographic". Appropriate correction is required.
13. Claim 30 is objected to because of the following informalities: "the number of digits of x ". Appropriate correction is required.
14. Claim 35 is objected to because of the following informalities: (where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$). The parenthesis should be removed for the limitation to be given patentable weight. Appropriate correction is required. **Please note that this is not a complete list of informalities.**
15. Claim 40 is objected to because of the following informalities: "**using an encipher function for asymmetric cryptographic**". Appropriate correction is required.
16. **Please note that this is not a complete list of informalities.**

Claim Rejections - 35 USC § 112

17. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
18. Claims 25-27, 29, 31-34, 37-39, and 42-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 25-27, 29, 31-34, 37-39, and 42-44 are dependent on cancelled claims. There is insufficient antecedent basis for these limitations in the claims.

19. Claims 23, 28, 35, and 40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 23, 28, 35, and 40 recite the limitations " $\alpha_1 \parallel \alpha_2 < q$ ". There is insufficient antecedent basis for these limitations in the claims.

20. Claims 24 and 40-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 24 and 40-41 recite the limitations "ciphertext and by using the secret key, α_1' , α_2' , m' where ". There is insufficient antecedent basis for these limitations in the claims.

21. Claim 30 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 30 recites the limitation " $m = D_K(C)$ " in page 9. There is insufficient antecedent basis for this limitation in the claim.

22. Claim 36 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 36 recites the limitation "transmitting ciphertext (u_1, u_2, v, \mathbf{C})" in page 13. There is insufficient antecedent basis for this limitation in the claim.

Art Unit: 2136

23. Claims 28, 40-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 28, 40-41 recite the limitation "... = $D_{sk}(e)$ ". There is insufficient antecedent basis for these limitations in the claims.

Claim Rejections - 35 USC § 101

24. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

25. Claims 23-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

26. Independent claims 23-24, 28, 30, 35-36, 40-41 are directed to an abstract idea. Abstract ideas are considered non-statutory subject matter. Dependent claims 25-26, 27, 29, 31-34, 37-39, 42-44 are rejected based on their dependency from claims 23-24, 28, 30, 35-36, 40-41.

27. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 103

28. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

29. Claims 23-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer.

Regarding claim 23, Cramer teaches a public-key cryptographic scheme comprising:

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
 - o G, G' : finite multiplicative group $G \subseteq G'$,
 - o q : prime number and the order of G ,
 - o $g_1, g_2 \in G$ (column 6, lines 1-67, column 7, lines 1-67),
 - o $c = g_1^{x_1} g_2^{x_2}, d_1 = g_1^{y_{11}} g_2^{y_{12}}, d_2 = g_1^{y_{21}} g_2^{y_{22}}, h = g_1^z$,
 - o $\pi : X_1 \times X_2 \times M \rightarrow G'$: one-to-one mapping
 - o $\pi^{-1} : \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
- where the group G is a partial group of the group G' , X_1 and X_2 are an infinite set of positive integers which satisfy:
 - o $\alpha_1 \parallel \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- where M is a plaintext space;
- a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1, \alpha_2 \in X_2, r \in Z_q$ for a plaintext m ($m \in M$), calculating:

Art Unit: 2136

- $u_1 = g_1^r$, $u_2 = g_2^r$, $e = \pi(\alpha_1, \alpha_2, m)h^r$, $v = g_1^{\alpha_1} c^r d_1^a r$ or $d_2^m r$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \parallel \alpha_2$ and transmitting (u_1, u_2, e, v) as a ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $m' \in M$) which satisfy:
 - $\pi(\alpha_1', \alpha_2', m') = e/(u_1^z)$ (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67) and if the following is satisfied:
 - $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_{11} + m' y_{21})})(u_2^{(x_2 + \alpha_2' y_{12} + m' y_{22})}) = v$
- outputting m' as the deciphered results (where $\alpha' = \alpha_1' \parallel \alpha_2'$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers ($x_1, x_2, y_1, y_2, z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 24, Cramer teaches a public-key cryptographic scheme comprising:

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
 - o p, q : prime number where q is a prime factor of $p-1$,
 - o $g_1, g_2 \in Z_p : \text{ord}_p(g_1) = \text{ord}_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
 - o $c = g_1^{x_1} g_2^{x_2} \text{ mod } p, d_1 = g_1^{y_{11}} g_2^{y_{12}} \text{ mod } p, d_2 = g_1^{y_{21}} g_2^{y_{22}} \text{ mod } p, h = g_1^z \text{ mod } p,$
 - o k_1, k_2, k_3 : positive constant, $10^{k_1+k_2} < q, 10^{k_3} < q, 10^{k_1+k_2+k_3} < p$ (column 7, lines 1-67)
- where a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ where $|\alpha_1| = k_1, |\alpha_2| = k_2$ for a plaintext m where $|m| = k_3$ where $|x|$ is the number of digits of x), calculating: $\tilde{m} = \alpha || K$
- selecting a random number $r \in Z_q$, calculating:
 - o $u_1 = g_1^r \text{ mod } p, u_2 = g_2^r \text{ mod } p, e = \tilde{m} h^r \text{ mod } p, v = g_1^{\alpha_1} c^r d_1^{\alpha_2} \text{ or } d_2^{\alpha_2} m^r \text{ mod } p$
- and transmitting (u_1, u_2, e, v) as a ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' where $|\alpha_1'| = k_1, |\alpha_2'| = k_2, |m'| = k_3$ which satisfy:

Art Unit: 2136

- $\alpha_1' || \alpha_2' || m' = e / (u_1^z) \bmod p$ (column 8, lines 1-67, column 9, lines 1-67, column 10, lines 1-67) and if the following is satisfied:
 - $(g_1^{\alpha_1'}) (u_1^{(x_1 + \alpha' y_{11} + m' y_{21})}) (u_2^{(x_2 + \alpha' y_{12} + m' y_{22})}) \equiv v \pmod p$
- outputting m' as the deciphered results, where $\alpha' = \alpha_1' || \alpha_2'$, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers ($x_1, x_2, y_1, y_2, z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 28, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
 - $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:
 - G, G' : finite multiplicative group $G \subseteq G'$,
 - q : prime number and the order of G ,

- $g_1, g_2 \in G$ (column 6, lines 1-67, column 7, lines 1-67),
 - $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^z$,
 - $\pi : X_1 \times X_2 \times M \rightarrow G'$: one-to-one mapping
 - $\pi^{-1} : \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
 - E : symmetric encipher function (column 12, lines 1-67)
- where the group G is a partial group of the group G' , X_1 and X_2 are an infinite set of positive integers which satisfy:
 - $\alpha_1 \parallel \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- where M is a key space;
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in \mathbb{Z}_q$ for key data K ($K \in M$), calculating:
 - $u_1 = g_1^r$, $u_2 = g_2^r$, $e = \pi(\alpha_1, \alpha_2, K)h^r$, $v = g_1^{\alpha_1} c^r d_1^{\alpha_2} d_2^{Kr}$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \parallel \alpha_2$, generating a ciphertext C of transmission data m by:
 - $C = E_K(m)$ (column 12, lines 1-35)
- by using a symmetric cryptographic function E and key data K , and transmitting (u_1, u_2, e, v, C) as the ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', K' ($\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $K' \in M$) which satisfy:
 - $\pi(\alpha_1' \parallel \alpha_2' \parallel K') = e/(u_1^z)$ (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67) and if the following is satisfied:

Art Unit: 2136

- $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha' y_{11} + K' y_{21})})(u_2^{(x_2 + \alpha' y_{12} + K' y_{22})}) = v$ where $\alpha' = \alpha_1' || \alpha_2'$,
- executing a decipher process by:
 - $m = D_{K'}(C)$
- outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers ($x_1, x_2, y_1, y_2, z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v).

Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 29, Cramer teaches wherein the ciphertext C is generated by:

- $C = E_K(f(\alpha_1, \alpha_2) || m)$
- by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:
 - $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha' y_{11} + K' y_{21})})(u_2^{(x_2 + \alpha' y_{12} + K' y_{22})}) = v$
 - $f(\alpha_1', \alpha_2') = [D_{K'}(C)]^K$

- where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x , and if the check passes, a decipher process is executed by:
 - o $m = [D_K(C)]^k$
- where $[x]^k$ indicates a bit train with the upper k bits of x being removed (column 8, lines 1-67, column 9, lines 1-67, column 12, lines 1-67).

Regarding claim 30, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in Z_q$ (column 7, lines 10-19)
- and a public-key:
 - o p, q : prime number, where q is a prime factor of $p-1$,
 - o $g_1, g_2 \in Z_p : \text{ord}_p(g_1) = \text{ord}_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
 - o $c = g_1^{x_1} g_2^{x_2} \bmod p, d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p, d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p, h = g_1^z \bmod p,$
 - o k_1, k_2, k_3 : positive constant $10^{k_1+k_2} < q, 10^{k_3} < q, 10^{k_1+k_2+k_3} < p$ (column 7, lines 1-67)
 - o E : symmetric encipher function (column 12, lines 1-35)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$, where $|\alpha_1| = k_1, |\alpha_2| = k_2$ for key data $K |K| = k_3$ where $|x|$ is the number of digits of x), calculating
- $\tilde{m} = \alpha || K$ (column 7, lines 1-67, column 8, lines 1-67, column 12, lines 1-67)

- selecting a random number $r \in Z_q$, calculating:
 - o $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $e = \tilde{m} h^r \bmod p$, $v = g_1^{\alpha_1} c^r d_1^{\alpha_2} \text{ or } d_2^{\alpha_2} K^r \bmod p$ (column 7, lines 1-67, column 8, lines 1-67)
- and generating a ciphertext C of transmission data by:
 - o $C = E_K(m)$ (column 12, lines 1-35)
- by using a symmetric cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', K' , where $|\alpha_1'| = k_1$, $|\alpha_2'| = k_2$, $|K'| = k_3$ which satisfy:
 - $\alpha_1' || \alpha_2' || K' = e / (u_1^z) \bmod p$ (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67)
 - and if the following is satisfied:
 - $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_{11} + K' y_{21})})(u_2^{(x_2 + \alpha_2' y_{12} + K' y_{22})}) \equiv v \pmod{p}$
 - where $\alpha' = \alpha_1' || \alpha_2'$,
 - executing a decipher process by:
 - o $m = D_{K'}(C)$
 - outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers $(x_1, x_2, y_1, y_2, z \in Z_q)$, generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v) .

Art Unit: 2136

Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 31, Cramer teaches wherein the ciphertext C is generated by:

- $C = E_K(f(\alpha_1, \alpha_2) || m)$
- by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:
 - o $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_{11} + K' y_{21})})(u_2^{(x_2 + \alpha_1' y_{12} + K' y_{22})}) \equiv v \pmod{p}$,
 - o $f(\alpha_1', \alpha_2') = [D_K(C)]^k$
- where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:
- $m = [D_K(C)]^{-k}$
- where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed (column 8, lines 1-67, column 9, lines 1-67, column 12, lines 1-67).

Regarding claim 35, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_1, y_2, z \in Z_q$ (column 7, lines 1-67)
- and a public-key:

- G, G' : finite multiplicative group $G \subseteq G'$,
 - q : prime number the order of G ,
 - $g_1, g_2 \in G$ (column 6, lines 1-67, column 7, lines 1-67),
 - $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$, $h = g_1^z$,
 - $\pi : X_1 \times X_2 \times M \rightarrow \text{Dom}(E)$: one-to-one mapping where $\text{Dom}(E)$ is the domain of the function E
 - $\pi^{-1} : \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
 - H : hash function (column 12, lines 1-35)
 - E : symmetric encipher function (column 12, lines 1-35)
- where the group G is a partial group of the group G' , X_1 and X_2 are an infinite set of positive integers which satisfy:
 - $\alpha_1 \parallel \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1, \alpha_2 \in X_2, r \in Z_q$, calculating:
 - $u_1 = g_1^r, u_2 = g_2^r, v = g_1^{\alpha_1} c^r d^{\alpha_2 r}, K = H(h^r)$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \parallel \alpha_2$, generating a ciphertext C of transmission data m by:
 - $C = E_K(\pi(\alpha_1, \alpha_2, m))$ (column 12, lines 1-35)
- by using a symmetric cryptographic function E ; and transmitting (u_1, u_2, v, C) as the ciphertext (column 8, lines 24-35); and
- a ciphertext reception and decipher step of calculating
 - $K' = H(u_1^z)$

Art Unit: 2136

- by using the secret key, calculating from the received ciphertext, α_1' , α_2' ,
(where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$) (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67) which satisfy:
 - o $\pi(\alpha_1', \alpha_2', m') = D_K(C)$
- if the following is satisfied:
 - o $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_1)})(u_2^{(x_2 + \alpha_1' y_2)}) = v$,
- where $\alpha' = \alpha_1' || \alpha_2'$,
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received cipher-text is rejected
(column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1 , x_2 , y_1 , y_2 , $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1 , u_2 , e , v).

Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 36, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_1, y_2, z \in Z_q$ (column 7, lines 1-67)

Art Unit: 2136

- and a public-key:
 - p, q : prime number (q is a prime factor of $p-1$),
 - $g_1, g_2 \in \mathbb{Z}_p : \text{ord}_p(g_1) = \text{ord}_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
 - $c = g_1^{x_1} g_2^{x_2} \bmod p, d = g_1^{y_1} g_2^{y_2} \bmod p, h = g_1^z \bmod p,$
 - k_1, k_2, k_3 : positive constant $10^{k_1+k_2} < q, 10^{k_3} < q, 10^{k_1+k_2+k_3} < p$ (column 7, lines 1-67)
 - H : hash function (column 12, lines 1-35)
 - E : symmetric encipher function where the domain of E is all positive integers (column 12, lines 1-35)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$, where $|\alpha_1| = k_1, |\alpha_2| = k_2$, where $|x|$ is the number of digits of x ,
- selecting a random number $r \in \mathbb{Z}_q$, calculating:
 - $u_1 = g_1^r \bmod p, u_2 = g_2^r \bmod p, v = g_1^{\alpha_1} c^r d^{\alpha_2} \bmod p, K = H(h^r \bmod p)$
- transmitting ciphertext (u_1, u_2, v, C) (column 8, lines 1-67)
- generating a ciphertext C of transmission data m by:
 - $C = E_K(\alpha_1 || \alpha_2 || m)$ (column 12, lines 1-35)
- by using a symmetric cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext (column 8, lines 1-67)
- a ciphertext reception and decipher step of calculating
 - $K' = H(u_1^z \bmod p)$

- by using the secret key, calculating from the received ciphertext, α_1' , α_2' ,
where $|\alpha_1'|=k_1$, $|\alpha_2'|=k_2$ which satisfy:
 - o $\alpha_1' || \alpha_2' || m' = D_K(C)$
- and if the following is satisfied:
 - o $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_1)})(u_2^{(x_2 + \alpha_2' y_2)}) \equiv v \pmod{p}$
- outputting m' as the deciphered results where $\alpha' = \alpha_1' || \alpha_2'$, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers ($x_1, x_2, y_1, y_2, z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 40, Cramer teaches a cryptographic communication method comprising:

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_1, y_2 \in Z_q$ (column 7, lines 1-67)
 - o sk : asymmetric cryptography decipher key (column 7, lines 1-67)

- and a public-key:
 - G : finite multiplicative group
 - q : prime number and the order of G ,
 - $g_1, g_2 \in G$ (column 6, lines 65-67, column 7, lines 1-10)
 - $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$,
 - $\pi : X_1 \times X_2 \times M \rightarrow \text{Dom}(E)$: one-to-one mapping where $\text{Dom}(E)$ is the domain of the function E
 - $\pi^{-1} : \text{Im}(\pi) \rightarrow X_1 \times X_2 \times M$ (column 7, lines 1-67)
 - $E_{pk}(\cdot)$: Encipher function for asymmetric cryptography (column 12, lines 1-35)
- where X_1 and X_2 are an infinite set of positive integers which satisfy:
 - $\alpha_1 \parallel \alpha_2 < q$ (for every $\alpha_1 \in X_1$, for every $\alpha_2 \in X_2$)
- where M is a plaintext space;
- a cipher-text generation and transmission step of selecting random numbers $\alpha_1 \in X_1, \alpha_2 \in X_2, r \in Z_q$, calculating:
 - $u_1 = g_1^r, u_2 = g_2^r, v = g_1^{\alpha_1} c^r d^{\alpha_2}$ (column 7, lines 1-67, column 8, lines 1-67)
- where $\alpha = \alpha_1 \parallel \alpha_2$, generating a ciphertext C of transmission data m by:
 - $e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$ (column 12, lines 1-35)
- by using an encipher function for asymmetric cryptographic E_{pk} , and transmitting (u_1, u_2, e, v) as the ciphertext (column 8, lines 24-35); and

Art Unit: 2136

- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1' , α_2' , m' , where $\alpha_1' \in X_1$, $\alpha_2' \in X_2$, $m' \in M$ which satisfy:
 - o $\pi(\alpha_1', \alpha_2', m') = D_{sk}(e)$ (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:
 - o $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_1)})(u_2^{(x_2 + \alpha_2' y_2)}) = v$
- where:
 - o $\alpha' = \alpha_1' || \alpha_2'$
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers (x_1 , x_2 , y_1 , y_2 , $z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1 , u_2 , e , v).

Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claim 41, Cramer teaches a cryptographic communication method comprising:

Art Unit: 2136

- a key generation step of generating a secret-key:
 - o $x_1, x_2, y_1, y_2 \in Z_q$ (column 7, lines 1-67)
 - o sk : asymmetric cryptography decipher key (column 7, lines 1-67)
- and a public-key:
 - o p, q : prime number where q is a prime factor of $p-1$
 - o $g_1, g_2 \in Z_p : \text{ord}_p(g_1) = \text{ord}_p(g_2) = q$ (column 6, lines 1-67, column 7, lines 1-67)
 - o $c = g_1^{x_1} g_2^{x_2} \text{ mod } p, d = g_1^{y_1} g_2^{y_2} \text{ mod } p,$
 - o k_1, k_2 : positive constant $10^{k_1+k_2} < q$
 - o $E_{pk}(\cdot)$: encipher function for asymmetric cryptography where the domain is all positive integers) (column 12, lines 1-35)
- a cipher-text generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$, where $|\alpha_1| = k_1, |\alpha_2| = k_2$ where $|x|$ is the number of digits of x , selecting a random number $r \in Z_q$, calculating:
 - o $u_1 = g_1^r \text{ mod } p, u_2 = g_2^r \text{ mod } p, v = g_1^{\alpha_1} c^r d^{\alpha_2} \text{ mod } p$
- generating a ciphertext C of transmission data m (positive integer) by:
 - o $e = E_{pk}(\alpha_1 || \alpha_2 || m)$ (column 12, lines 1-35)
- by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext (column 8, lines 1-67); and
- a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α_1', α_2', m' where $|\alpha_1'| = k_1, |\alpha_2'| = k_2, m'$ is a positive integer which satisfy:

- $\alpha_1' || \alpha_2' || m' = D_{sk}(e)$ (column 8, lines 36-67, column 9, lines 1-67, column 10, lines 1-67)
- and if the following is satisfied:
 - $(g_1^{\alpha_1'})(u_1^{(x_1 + \alpha_1' y_1)})(u_2^{(x_2 + \alpha_1' y_2)}) = v \pmod{p}$,
- where
 - $\alpha' = \alpha_1' || \alpha_2'$
- outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected (column 9, lines 1-67, column 10, lines 1-67, column 11, lines 1-67).

Cramer discloses generating a secret-key using five exponent numbers ($x_1, x_2, y_1, y_2, z \in Z_q$), generating a public-key, and transmitting a cipher-text (u_1, u_2, e, v). Furthermore, Cramer teaches generating extended private key and public key (column 4, lines 19-45). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step. One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme (Cramer, column 3, lines 1-67, column 4, lines 1-67).

Regarding claims 25, 32, 37, and 42, Cramer teaches wherein the public-key is generated by a receiver and is made public (columns 1-3).

Regarding claims 26 and 33, Cramer teaches wherein in said ciphertext transmission step, the random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, and $r \in Z_q$ are selected

Art Unit: 2136

beforehand and the following is calculated and stored beforehand: $u_1 = g_1^r$, $u_2 = g_2^r$, h^r , $g_1^{\alpha_1} c^r d_1^{\alpha_2 r}$ (column 7, lines 1-67, column 8, lines 1-67).

Regarding claims 27 and 34, Cramer teaches wherein in said ciphertext transmission step, the random numbers α_1 , α_2 where $|\alpha_1| = k_1$, $|\alpha_2| = k_2$, and $r \in \mathbb{Z}_q$ are selected beforehand and the following is calculated and stored beforehand: $u_1 = g_1^r \bmod p$, $u_2 = g_2^r \bmod p$, $h^r \bmod p$, $g_1^{\alpha_1} c^r d_1^{\alpha_2 r} \bmod p$ (column 7, lines 40-67, column 8, lines 1-22).

Regarding claims 38 and 43, Cramer teaches wherein in said ciphertext transmission step, the random numbers α_1 , α_2 , where $\alpha_1 \in X_1$, $\alpha_2 \in X_2$ and $r \in \mathbb{Z}_q$ are selected beforehand and the u_1 , u_2 , e , and v (u_1 , u_2 , and v) are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Regarding claims 39 and 44, Cramer teaches wherein in said ciphertext transmission step, the random numbers α_1 , α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \in \mathbb{Z}_q$ are selected beforehand and the u_1 , u_2 , e , and v (u_1 , u_2 , and v) are calculated and stored beforehand (column 7, lines 40-67, column 8, lines 1-22).

Conclusion

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent Number: 6,081,598 to Dai, for "a cryptography system improves the decryption speed in the RSA algorithm by taking advantage of certain subgroups of Z_n^* . The cryptography system employs a new family of trapdoor permutations based on exponentiation in subgroups of Z_n^* ". Abe (Japan Patent 2000-216774) teaches generating a secret key and a public key.

31. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-

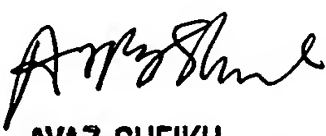
Art Unit: 2136

5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

33. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

34. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100